

AO 91 (Rev. 02/09) Criminal Complaint

# United States District Court

for the  
Western District of New York



United States of America

v.

Case No. 21-mj-5017

SHAWN JOHNSON

*Defendant*

## CRIMINAL COMPLAINT

I, MICHAEL HOCKWATER, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of December 2, 2019, in the Western District of New York and elsewhere, the defendant knowingly possessed material that contained an image of child pornography that has been transported using any means and facility of interstate and foreign commerce, including by computer, or that had been produced using materials that had been mailed, shipped, or transported in or affecting interstate and foreign commerce by any means, including by computer.

**In violation of Title 18, United States Code, Section 2252A(a)(5)(B).**

On or about December 2, 2019, in the Western District of New York and elsewhere, the defendant knowingly altered, destroyed, or mutilated a record, document, or tangible object with the intent to impede or obstruct this investigation.

**All in violation of Title 18, United States Code, Section 1519.**

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

*Complainant's signature*

MICHAEL HOCKWATER  
TASK FORCE OFFICER  
FEDERAL BUREAU OF INVESTIGATION

*Printed name and title*

Sworn to telephonically.

Date: February 8, 2021

*Judge's signature*

City and State: Buffalo, New York

HONORABLE MICHAEL J. ROEMER  
UNITED STATES MAGISTRATE JUDGE

*Printed name and title*

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     SS:  
CITY OF BUFFALO        )

I, MICHAEL HOCKWATER, being duly sworn, depose and say:

1. I am a Police Detective with the Town of Cheektowaga, New York Police Department. I have been a Police Officer since August of 1989. I am currently assigned as a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI"), Buffalo Field Office, Child Exploitation Task Force, which targets individuals involved in the online sexual exploitation of children. I have been a TFO since June 14, 2010. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers and electronic media are used as the means for receiving, transmitting, and storing child pornography.

2. I make this affidavit in support of a criminal complaint charging **SHAWN JOHNSON ("JOHNSON")**, born February 23, 1987, with the violation of Title 18 United States Code Sections 2252A(a)(5)(B) [Possession of Child Pornography] and 1519 [Destruction of Evidence].

3. The statements contained in this affidavit are based on my involvement in this investigation, as well as information provided to me by other law enforcement officers in this investigation, and upon my training and experience as a TFO of the FBI. Because I offer this affidavit for the limited purpose of seeking a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause to believe that **JOHNSON** knowingly violated Title 18, United States Code, Sections 2252A(a)(5)(B) and 1519.

#### **PROBABLE CAUSE**

4. This investigation involves a user of a particular Internet-based, peer-to-peer (“P2P”) network (“Network”) that allows users to anonymously share files, chat on message boards, and access websites within the Network. The Network can be used to advertise and distribute images and videos of child pornography. Law enforcement has been investigating child pornography trafficking by users of the Network since at least 2011.

5. This Network, unlike other file sharing systems, does not provide a search function for its users whereby users can insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from the Network must obtain the key associated with a particular child pornography file and then use that key to download the file.

6. On Friday, September 6, 2019, while reviewing data received by law enforcement Network computers, a colleague of mine observed IP address 67.247.212.12, with the Network Location ID 0.101859926262521, requesting blocks of suspected child

pornography files on three dates discussed in greater detail below, at paragraphs 9 through 14. The files were suspected child pornography files because the keys for the files were keys known to be associated with child pornography files. While it is not an absolute certainty the user was the original requestor, with respect to each file, considering the number of requested blocks, the total number of blocks required to assemble the file, and the number of peers the user had, the number of requests for blocks of the file is significantly more than one would expect to see if the user of IP address 67.247.212.12 were merely routing the request of another user.<sup>1</sup>

7. Accordingly, based on my review of those records, my understanding of the Network, my training and experience, and the fact that the same user requested pieces of multiple child pornography files, I believe that there is probable cause to believe that the user of IP address 67.247.212.12 was the original requestor of each of these files.

8. Between Friday, August 23, 2019 at 10:27 PM UTC and Friday, August 23, 2019 at 10:42 PM UTC, a computer running Network software with an IP address of 67.247.212.12, with an average of 32.6 peers, requested from a law enforcement computer 60 out of 1,699 required pieces (or “blocks”) needed to assemble a file with a SHA1 digital hash value of 2DUW7YMWJ3B5O2HX6K5GN4HWNDSN4ZCX.

- a. The key associated with this file, which the requesting user had to obtain and enter in order to download the file, is:

---

<sup>1</sup>. A detailed explanation of how the P2P network operates, and how users obtain child pornography using it, is included in paragraphs 5 through 53 of the affidavit I submitted in support of my application for a search warrant in this matter, which I incorporate by reference here. *Matter of Search of 257 Angle Road, West Seneca, New York 14224*, 20-MJ-5302 (MJR) (filed under seal).

CHK@hPCI29eJuZOFH1QiUIfPYHWGLw12tyBlp9yIg1e5xnM,p~MfELE  
K8VDQ8j2jP7nMHcDqXxbW-eKUEfeMlaautsw,AAMC--8/D3844.avi.

- b. A law enforcement officer downloaded the exact same file with the above referenced SHA1 hash value from the P2P network. It is a video titled "D3844.avi"
  - c. The video is approximately four minutes and fifteen seconds long. In the video, a minor female approximately 10 years old is dancing in front of the camera removing her clothing until she is completely naked. The minor child is observed touching her vagina and anus with her fingers. Based on my training and experience, I believe that the video contains child pornography as defined by 18 U.S.C. § 2256(8).
9. Between Thursday, August 29, 2019 at 2:51 AM UTC and Thursday, August 29, 2019 at 2:52 AM UTC, a computer running Network software with an IP address of 67.247.212.12, with an average of 41.0 peers, requested from a law enforcement computer 68 out of 912 required pieces (or "blocks") needed to assemble a file with a SHA1 digital hash value of CQ4QZCBFLMQI34UYZ63EBPO7RKGFEREI.
  - a. The key associated with this file, which the requesting user had to obtain and enter in order to request the file is: CHK@ILZvdJWeG66ubZHz-x3pgXdNLhTo4HLLZ8f7~8Os4MM,iLjor5TfrovUGAXlx-SOfE0ILtw9o5HDaWs97K9HM3w,AAMC--8/2Dancer.avi.
  - b. A law enforcement officer downloaded the exact same file with the above referenced SHA1 hash value from the P2P network. It is a video titled "2dancer.avi".
  - c. The video is approximately 5 minutes and seventeen seconds long. In the video, a minor female approximately 8 years old is dancing in front of the camera removing her clothing until she is completely naked. The minor female is observed touching and rubbing her vagina with her fingers. Based on my training and experience, I believe that the video contains child pornography as defined by 18 U.S.C. § 2256(8).
10. Between Wednesday, August 28, 2019 at 1:11 AM UTC and Wednesday, August 28, 2019 at 2:44 AM UTC, a computer running Network software with an IP address of 67.247.212.12, with an average of 42.4 peers, requested from a law enforcement computer

105 out of 3,804 required pieces needed to assemble a file with a SHA1 digital hash value of UTQTILKTON34YNCSX4POLAHDDOF36PTS.

- a. The key associated with this file, which the requesting user had to obtain and enter in order to request the file, is: CHK@RH60ivbo6l~d2VB6RcUWfYj1kfJiSw3ZjRgZqiAKJ~w,rF5aXEvaROcQcCKFIyN~7~NY2MeXma808zq9FuFm42c,AAMC--8/Stickam%20Yogirl-12Yo-Fat-Girl-Self-Masturbating-Pussy-With-Fingers-Introducing-Candle-In-Pussy-Real-Sound-Hq-06m13S.avi.
- b. A law enforcement officer downloaded the exact same file with the above referenced SHA1 hash value from the network. It is a video titled "Stickam Yogirl-12Yo-Fat-Girl-Self-Masturbating-Pussy-With-Fingers-Introducing-Candle-In-Pussy-Real-Sound.avi."
- c. The video is approximately six minutes and thirteen seconds long. In the video, a minor female approximately 12 years old, removes her clothing and masturbates in front of the camera using her hands. The female also inserts a plastic cylindrical object into her vagina. Based on my training and experience, I believe that the video contains child pornography as defined by 18 U.S.C. § 2256(8).

11. The fact that the user at IP address 67.247.212.12 requested pieces associated with a particular file on the network indicates that the user attempted to download the file's contents from the P2P network. It does not indicate whether the user successfully retrieved all of the necessary pieces to successfully download the file.

12. Using publicly available search tools, law enforcement determined that IP address 67.247.212.12 was controlled by Internet Service Provider ("ISP") Charter Communications.

13. On or about September 13, 2019, an FBI administrative subpoena was served on Charter Communications for subscriber information relating to the use of IP address 67.247.212.12 on August 23, 2019 at 5:27 PM, Eastern and August 28, 2019 at 9:51 PM,

Eastern. A review of the results obtained revealed the subscriber was James Johnson, 257 Angle Road West Seneca, New York 14224.

14. Based on the aforementioned information, I obtained a federal search warrant for 257 Angle Road, West Seneca, New York 14224 (*See Matter of the Search of 257 Angle Road, West Seneca, New York 14224*, 20-MJ-5302 (MJR) (filed under seal)). On December 2, 2019, agents from the Buffalo Division of the FBI along with Task Force Officers conducted a search of the residence pursuant to the search warrant.

15. As I entered the residence I heard loud noises coming from the second floor. I ascended the stairs to the second floor and encountered SHAWN JOHNSON standing in his bedroom with a laptop computer in his hands smashing it against the wall trying to damage it. The laptop was an ASUS Laptop bearing serial number G1N0GR02E74502C with a Seagate 500GB hard drive bearing serial number SBY1NVAF installed in it. The Seagate 500GB hard drive is labeled "Made in China."

16. The laptop suffered serious damage due to JOHNSON's actions and had to be sent to the FBI's Digital Forensics Analysis Unit Laboratory for repair. The Seagate 500GB hard drive bearing serial number SBY1NVAF was repaired and approximately 80% of the data was recovered and transferred to a derivative hard drive. The derivative hard drive was returned to the Western New York Regional Computer Forensics Laboratory ("WNYRCFL") for analysis.



17. The WNYRCFL provided me with the results of the forensic examination of the derivative hard drive. The key files for the three videos discussed in paragraphs 9, 10 and 11 that depict child pornography were found on the hard drive.

18. Based on the WNYRCFL forensic examination, I discovered of at least 100 video files and 800 image files that contain child pornography as defined in 18 U.S.C. § 2256 on the hard drive. For example:

- a. A 24-second long video titled “(pthc) new 2016 Pedo Childlover 8yo Daddy’s Little Girl JM 08.mp4” wherein an adult male is observed inserting his penis into the vagina of a minor female under the age of 10. The male appears to ejaculate on the child’s vagina.
- b. A 15-second long video titled “3yo cute face” wherein an adult male is masturbating and ejaculating on the face of a blind folded naked minor female under the age of 5.
- c. A 4 minute and 1 second video titled “dog(-)2017\_2649” wherein a female under the age of 10 rubs a substance on her vagina while a dog licks it off.

## **II. CONCLUSION**

19. Based upon the above information, I submit that there is probable cause to believe that, on December 2, 2019, in the Western District of New York, **SHAWN JOHNSON** knowingly possessed material that contained an image of child pornography that has been transported using any means and facility of interstate and foreign commerce, including by computer, or that had been produced using materials that had been mailed, shipped, or transported in or affecting interstate and foreign commerce by any means, including by computer, in violation of Title 18, United States Code, Section 2252A(a)(5)(B), and that he knowingly altered, destroyed, or mutilated a record, document, or tangible object



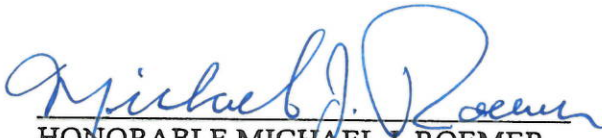
with the intent to impede or obstruct this investigation in violation of Title 18, United States Code, Section 1519.



MICHAEL HOCKWATER  
Task Force Officer  
Federal Bureau of Investigation

Sworn and subscribed telephonically

this 8<sup>th</sup> day of February, 2021.



HONORABLE MICHAEL J. ROEMER  
United States Magistrate Judge